

DOCTORAL THESIS

Biometric system security and privacy: data reconstruction and template protection

Mai, Guangcan

Date of Award:
2018

[Link to publication](#)

General rights

Copyright and intellectual property rights for the publications made accessible in HKBU Scholars are retained by the authors and/or other copyright owners. In addition to the restrictions prescribed by the Copyright Ordinance of Hong Kong, all users and readers must also observe the following terms of use:

- Users may download and print one copy of any publication from HKBU Scholars for the purpose of private study or research
- Users cannot further distribute the material or use it for any profit-making activity or commercial gain
- To share publications in HKBU Scholars with others, users are welcome to freely distribute the permanent URL assigned to the publication

Abstract

Biometric systems are seeing increasing use, from daily entertainment to critical applications such as security access and identity management. Biometric systems should thus meet the stringent requirement of a low error rate. In addition, for critical applications, biometric systems must address security and privacy issues. Otherwise, severe consequences may result, such as unauthorized access (security) or the exposure of identity-related information (privacy). It is therefore imperative to study vulnerability to potential attacks and identify the corresponding risks. Furthermore, countermeasures should be devised and patched on the systems.

In this thesis, we study security and privacy issues in biometric systems. We first attempt to reconstruct raw biometric data from biometric templates and demonstrate the security and privacy issues caused by data reconstruction. We then make two attempts to protect biometric templates from reconstruction and improve the state-of-the-art biometric template protection techniques.

To summarize, this thesis makes the following contributions.

- **Data Reconstruction:** An investigation of the invertibility of face templates generated by deep networks. To the best of our knowledge, this is the first such study of the security and privacy of face recognition systems.
- **Template Protection:** An end-to-end method for simultaneous extraction and

protection of templates given raw biometric data (e.g., face images). To the best of our knowledge, this is the first end-to-end method for the direct generation of secure templates from raw biometric data.

- **Template Protection:** A binary fusion approach for multi-biometric cryptosystems to offer accurate and secure recognition. The proposed fusion approach can simultaneously maximize the discriminability and entropy of the fused binary output.

Keywords: biometric template, biometric security, data reconstruction, template reconstruction, and template protection

Table of Contents

| | |
|---|-------------|
| Declaration | i |
| Abstract | ii |
| Acknowledgements | iv |
| Table of Contents | ix |
| List of Tables | xi |
| List of Figures | xvii |
| 1 Introduction | 1 |
| 1.1 Biometric System | 1 |
| 1.1.1 Biometric Recognition System | 2 |
| 1.1.2 Security and Privacy Concerns | 4 |

| | | |
|----------|--|-----------|
| 1.2 | Data Reconstruction and Template Protection | 6 |
| 1.2.1 | Data Reconstruction | 6 |
| 1.2.2 | Template Protection | 7 |
| 1.3 | Contributions of This Thesis | 10 |
| 1.4 | Thesis Overview | 12 |
| 2 | Reconstructing Face Images from Deep Face Templates | 14 |
| 2.1 | Introduction | 14 |
| 2.2 | Related Work | 18 |
| 2.2.1 | Reconstructing Face Images from Deep Templates | 18 |
| 2.2.2 | GAN for Face Image Generation | 20 |
| 2.3 | Proposed Template Security Study | 21 |
| 2.3.1 | Template Reconstruction Attack | 21 |
| 2.3.2 | <i>NbNet</i> for Face Image Reconstruction | 25 |
| 2.3.3 | Reconstruction Loss | 27 |
| 2.3.4 | Generating Face Images for Training | 28 |
| 2.3.5 | Differences with <i>DenseNet</i> | 32 |
| 2.3.6 | Implementation Details | 32 |

| | | |
|----------|---|-----------|
| 2.4 | Performance Evaluation | 35 |
| 2.4.1 | Database and Experimental Setting | 35 |
| 2.4.2 | Verification Under Template Reconstruction Attack | 39 |
| 2.4.3 | Identification with Reconstructed Images | 47 |
| 2.4.4 | Computation Time | 49 |
| 2.5 | Summary | 50 |
| 3 | Secure Deep Biometric Template | 51 |
| 3.1 | Introduction | 51 |
| 3.2 | Related Work | 53 |
| 3.2.1 | Template Protection Schemes | 53 |
| 3.2.2 | Fuzzy Commitment Scheme | 54 |
| 3.3 | Proposed Secure Template Generation | 56 |
| 3.3.1 | Secure System Construction | 56 |
| 3.3.2 | Randomized CNN | 58 |
| 3.3.3 | Secure Sketch Construction | 63 |
| 3.3.4 | Loss Function for Training | 65 |
| 3.3.5 | Network Architecture | 68 |

| | | |
|----------|--|-----------|
| 3.4 | Performance Evaluation and Analysis | 69 |
| 3.4.1 | Experimental Setting | 69 |
| 3.4.2 | Matching Accuracy of the Randomized CNN | 73 |
| 3.4.3 | Unlinkability Analysis | 73 |
| 3.4.4 | Trade-off between Matching Accuracy and Security | 75 |
| 3.5 | Summary | 80 |
| 4 | Binary Feature Fusion for Multi-biometric Cryptosystems | 82 |
| 4.1 | Introduction | 82 |
| 4.2 | Review on Binary Feature Fusion | 85 |
| 4.3 | The Proposed Binary Feature Fusion | 88 |
| 4.3.1 | Overview of the Proposed Method | 88 |
| 4.3.2 | Dependency Reductive Bit-group Search | 89 |
| 4.3.3 | Discriminative Within-group Fusion Search | 92 |
| 4.3.4 | Discussion and Analysis | 94 |
| 4.4 | Performance Evaluation | 97 |
| 4.4.1 | Database and Experiment Setting | 97 |
| 4.4.2 | Evaluation Measures for Discriminability and Security | 100 |

| | | |
|----------|---|------------|
| 4.4.3 | Discriminability Evaluation | 102 |
| 4.4.4 | Security Evaluation | 104 |
| 4.4.5 | Robustness of Varying Qualities of Biometric Inputs | 105 |
| 4.4.6 | Trade-off between Discriminability and Security | 108 |
| 4.5 | Summary | 108 |
| 5 | Conclusions and Future Research | 111 |
| 5.1 | Conclusions | 111 |
| 5.2 | Future Research Directions | 112 |
| | Appendics | 114 |
| | Bibliography | 133 |
| | Curriculum Vitae | 135 |